Attorney's Docket No. 1030681-000291

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP: APPEAL BRIEF**
A-jung Kim	Group Art Unit: 2135
Application No.: 09/816,080	Examiner: BEEMNET W. DADA
Filed: March 26, 2001	Appeal No.: _____
For: KEY AGREEMENT METHOD IN SECURE COMMUNICATION SYSTEM USING MULTIPLE ACCESS METHOD	

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated April 6, 2006 (Paper No. 033006), finally rejecting claims 1-6, which are reproduced as the Claims Appendix of this brief.

☐ A check covering the ☐ $250 ☐ $500 Government fee is filed herewith.

☒ Charge ☐ $250 ☒ $500 to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

I. Real Party in Interest

The present application is assigned to Samsung Electronic Co., Ltd. Samsung Electronic Co., Ltd. is the real party in interest, and is the assignee of Application No. 09/816,080.

II. Related Appeals and Interferences

The Appellant legal representative, or assignee, does not know of any other appeal or interferences which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III. Status of Claims

All of the pending claims, claims 1-6, are pending and were rejected in the final Office Action of April 6, 2006.

IV. Status of Amendments

No amendments have been filed subsequent to the final Office Action.

V. Summary Claimed Subject Matter

By way of a concise explanation of the claimed subject matter of the only independent claim, claim 1, Appellants offer the following comments, wherein bracketed numbers refer to the paragraph numbers of the present application.

Claim 1 recites a key agreement method for secure communication in a multiple access system. [0001] In cryptographic systems, a key is used as an input of an encryption or decryption function that serves to scramble data. [0002] Generally the ciphered text and the encryption algorithms are available on public communication channels, and both legitimate and illegitimate users can access them. [0003] It is therefore important to distribute, store and manage security keys so that only legitimate uses can access them. [0003] Overall security depends on the security of the keys. [0003]

Cryptosystem algorithms are vulnerable to attack by powerful computers. One of the drawbacks of conventional cryptosystems is that communications can be monitored without legitimate users being aware that any eavesdropping is taking place. [0004] The eavesdropper may then be able to, without detection, obtain the value of the key by tapping or cloning the transmitted key signals and through signal

manipulation legitimate users cannot be sure whether the communication line has been attacked or when eavesdropping occurs. [0004]

As opposed to encryption systems that depend upon computational complexity, new cipher systems are based on key distribution systems using quantum cryptology. [0006] But there are difficulties in distributing keys through quantum states. [0006]

Embodiments of the present invention include ways of attaining secure communication due in part to providing a key agreement method for secure communication in a multiple access system. As disclosed in paragraph [0007], ways are provided to detect the extent of eavesdropping and thus make an eavesdropper's attempts more futile. Within the scope of the present invention, this can be done in certain embodiments at the physical layer without modifying the configurations and topographies of the communication system. [0007]

The key agreement method of the present invention in cryptosystems not only can prevent an eavesdropper from obtaining the correct value of the secret key agreed between the users, but also can enable determining whether eavesdropping is taking place and estimates the degree of eavesdropping. The former function can fulfilled by making the eavesdropping have uncorrelated measurement results that can be seen by the legitimate user by using detector noise and intermodulation noise or cross-talk generated from the other channels in a multiple access system such as a code division multiple access (CDMA) system and a wavelength division multiple access (WDMA) system. The second function can be achieved by estimating a degree of contamination created by the eavesdropper s tapping and retransmittiing the bits. [0017]

The key agreement method of claim 1 includes five steps, steps (a)-(e).

(a) a first user encoding a signal from a source by a bit sequence and transmitting the signal;

The general communication structure shown in FIG. 1 can be used as a cryptosystem configuration of the presently claimed invention in distributing a secret key. In this exemplary embodiment, the user on a transmitting side, who is the generator of the key, modulates a signal from a source with an encoder (or

modulator) 102 to produce a sequence of arbitrary bits independently of users on other channels and transmits the modulated signal. The signals from the users on a transmitting side are combined by the multiplexer (or coupler) 104 and then transmitted via the same shared transmission medium. [0019]

FIG. 5 is a flowchart for illustrating a key agreement protocol in a communication system according to the present invention. [0030]

Referring to FIG. 5, the first user, modulates the signal from a source to an sequence of arbitrary bits with the encoder and with, for instance, phase reverse keying and transmits the modulated signal (step 500). [0032]

(b) a second user who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal;

The signal is then split by the demultiplexer (or splitter) 120, filtered to have its own channel while passing through the corresponding encoders (or demodulator) 122, and detected by the N detectors 124 in this exemplary embodiment. The detector 124 is affected by intermodulation noise caused by the signals of other channels as well as detector s intrinsic noise such as thermal noise, short noise, and electric noise. [0020]

FIG. 2 is a block diagram showing the structures of encryption and decryption with a secret private key shared between users in a general cryptosystem in an exemplary embodiment. [0021]

FIGS. 3A and 3B show examples of realizing an encoder and a decoder in the cryptosystem employing optical code division multiple access (CDMA). [0023]

FIGS. 4A through 4D show pulse signal patterns at each position in a time delayed CDMA system as an exemplary system which the present invention can be applied. [0029]

Referring to FIG. 5, the second user receives and filters the transmitted signal with the decoder matching to the encoder of the first user and measures the value of bits received by the detector (step 502). The signal transmitted in step 500 is a weak signal susceptible to noise. The measured values of received bits in step 502 has

spreading distribution around the real value of the transmitted signal due to intermodulation noise or cross-talk, background noise, and device noise. [0032]

(c) the second user adopting only bits, on a bit-by-bit basis, having the measured value beyond the threshold value which is predetermined;

Referring to FIG. 5, the second user adopts as a key only bits having the value beyond a threshold value which was determined in advance and discard the bits falling in the erroneous region below the threshold (step 504). [0033]

(d) the second user informing the first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits;

Referring to FIG. 5, the second user informs the first user that the bits adopted as the key is the n-th bits, without telling their values (step 506). [0033]

(e) the first and second users taking the adopted bits as a key string, and discarding the remaining bits.

Referring to FIG. 5, the users, the first user and the second user, take the adopted bits as the key string, based on their measurement (step 508). [0033]

In case of the presence of eavesdropping, the eavesdropper s erroneous decisions and retransmissions introduce errors in the bit string of the second user. If the error rate exceeds a tolerable value, it is supposed that there is a possibility of eavesdropping and the transmission is considered unsafe. Thus, the key string is to be discarded and the users have to perform the key agreement process again, returning to step 500. [0034]

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1-6 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,678,379 to Mayers et al. ("Mayers").

VII. Argument

"To anticipate, every element and limitations of the claimed invention must be found in a single prior art reference, arranged as claimed." *Brown v. 3M*, 265 F.3d 1349, 60 USPQ 2d 1375 (Fed. Cir. 2001).

Mayers discloses a method for testing the security of a quantum cryptographic system used for quantum key distribution. The Mayers method utilizes the polarization states of photons, with the photons possessing quantum states satisfying certain relationships between three bases (Mayers, col. 7, line 67 – col. 8, line 20).

The Mayers' method involves a sending party producing a set of three photons in a GHZ state from a GHZ source in a predetermined base. The sending party uses prearranged measurement bases to measure the first and second of the three photons. The third photon is transmitted to the receiving party through a quantum channel, and a receiving party uses a prearranged measurement bases to measure the transmitted photon. The parity of the measurement results for the three photons are collated on a bitwise basis between the sending and receiving parties, and a check is made as to whether or not the parity is correct. After a sufficiently large number of tests have been conducted, it is determined that the quantum key distribution apparatus can be relied upon if the error rate is within a tolerable range (Mayers, col. 8, line 46 – col. 9, line 7).

If the apparatus is found to be reliable, then key distribution is performed in Mayers by the sending party again producing a set of three photons in a GHZ state from a GHZ source in a predetermined base. The sending party measures the first and second of these photons using bases selected from two other predetermined bases at random for each bit, and stores the measurement bases and the results. The third photon is transmitted to the receiving party through the quantum channel,

and the receiving party measures the transmitted photon using a base selected from two other predetermined bases at random for each bit, and also stores the measurement bases and the result. The three bases used are then collated between the sending and receiving parties for each bit without telling the measurement results. Of these, it is approximated that half of the bits will correspond to cases where the selected bases constitutes one of four predetermined bases, and these bits are kept and the others are discarded (Mayers, col. 9, lines 8-28).

In Mayers, the sending party and receiving party also extract test bits at random and check whether or not they are correct by collating the parity of the bit values for each bit. If this test produces correct parities for a sufficient number of bits, Mayers concludes that there is no eavesdropping activity, and the test bits are discarded and a shared key is produced from the remaining random series of bits (Mayers, col. 9, lines 29-41).

The presently claimed invention concerns a key arrangement method including a first system which encodes a bit sequence and sends it to a second system. The second system decodes the received signals and measures the signal values. In contrast to the Meyers system, in the presently claimed invention, the second system records some second values, which are above a predetermined value, and tells the first system **bit positions** of the selected bits. The first system selects values corresponding to those bit positions, and discards the rest of them.

In comparing the present invention to Mayers, it is clear that Mayers does not adopt only bits having a measured value beyond a threshold value. As disclosed in Mayers, if a sufficient number of bits meet a parity test, it is concluded that there is no eavesdropping activity. The bits that have been tested are discarded, and a shared key is produced from the remaining random series of bits (Mayers, col. 9, lines 29-36). In contrast, and as recited in claim 1, the second system adopts only those bits having a measured value beyond the threshold value, and informs the first system of the bit positions of the selected bits. The adopted bits are then used as a key string for the first and second systems. Mayers discloses instead to discard the

bits that are actually tested, and utilize the remaining random series of bits to form the shared key.

Further, in the present invention, it is the second system that determines which bits to use for the key string. In contrast, Mayers discloses that the parity of the measurement results are collated on a bitwise basis between the sending and receiving parties. Thus, both the sending and receiving parties in Mayers are involved in the testing procedure.

Accordingly, for at least the above-identified reasons, Appellant submits that claim 1 is allowable over Mayers.

The dependent claims add features which further remove the present invention from the applied art. For instance, claim 2 recites that if the transmission is considered safe, the key string is accepted and refined, for instance. The Examiner cites column 8, lines 65 through column 9, lines 20, but the undersigned could not find any teaching of the combination of features of claim 2. Similarly, support could not be found for the Examiner's assertion that column 8, lines 46-60 taught the recitations of claim 4, particularly since there was no mention of noise, let alone mutual modulated noise, by another transmitter.

Likewise, column 6, lines 30-32 or column 9, lines 1-10 do not teach or disclose the recitations of claims 5 and 6 regarding the second user determining the threshhold value of step c, considering at least three factors; transmission rate, transmission error rate and degree of security.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

See attached Evidence Appendix for copies of evidence relied upon by Appellant.

X. Related Proceedings Appendix

See attached Related Proceedings Appendix for copies of decisions identified in Section II, supra.

In light of the foregoing comments pointing to features of the pending claims not found in the applied art, Appellants respectfully request that the Examiner's rejection be overturned and the application returned to the examining corps for prompt allowance.

Respectfully submitted,

Buchanan Ingersoll PC

Date: June 19, 2006

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, VA 22313-1404
703.836.6620

Table of Contents

III. CLAIMS APPENDIX

The Appealed Claims

1. A key agreement method for secure communication in a multiple access system, the key agreement method comprising the steps of:

(a) a first user encoding a signal from a source by a bit sequence and transmitting the signal;

(b) a second user who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal;

(c) the second user adopting only bits, on a bit-by-bit basis, having the measured value beyond the threshold value which is predetermined;

(d) the second user informing the first user that the bits adopted are the

n-th bits in the transmitted bit sequence, not telling the values of the bits; and

(e) the first and second users taking the adopted bits as a key string, and discarding the remaining bits.

2. The method of claim 1, further comprising the steps of:

(f) selecting a subset of bits from the key string shared by the first and second users and checking errors;

(g) if the error rate obtained in (f) is below a tolerable level, considering the transmission safe, accepting the key string and obtaining a refined key string with amplification such as error correction process; and

(h) discarding the key adopted in the step (e) if the error rate obtained in (f) exceeds the tolerable level, returning to the step (a) and performing (a) through (f) until getting the key string which satisfies the condition (g).

3. The method of claim 1, wherein the signal transmitted in step (a) is susceptible to noise.

4. The method of claim 1, wherein the second user uses a receiver affected by mutual modulated noise by another transmitter.

5. The method of claim 1, wherein the threshold value of the step (c) is determined by the second user considering at least a transmission rate, a transmission error rate, and a degree of security.

6. The method of claim 4, wherein the threshold value of the step (c) is determined by the second user considering at least a transmission rate, a transmission error rate, and a degree of security.

IX. EVIDENCE APPENDIX

None submitted.

X. RELATED PROCEEDINGS APPENDIX

None identified.